

Przedmowa (9)

Wstęp (11)

- Czym jest cracking (12)
- Ogólne zasady ochrony przed crackiem (13)
 - o Zasady Marka (13)
 - o Kolejne zasady (14)
- Podstawowe programy używane do crackingu (15)
- Czy w ogóle zabezpieczanie oprogramowania ma sens ("I tak ktoś to scrackuje") (16)
- Zawartość płyty CD (16)

Rozdział 1. Istniejące sposoby zabezpieczeń i ich podatność na ataki (17)

- Szyfrowanie danych (17)
- Programy niepełne (18)
 - o Podstawowa klasyfikacja dzisiejszych typów zabezpieczeń (18)
 - Ograniczenia czasowe (19)
 - Kolejne ograniczenia ilościowe (22)
 - Numer seryjny (22)
 - Plik klucza (27)
 - Programy z ograniczoną funkcjonalnością (32)
 - Klucz sprzętowy (34)
 - Kontrola obecności płyty CD (36)
 - o Zabezpieczenia przed kopiowaniem płyt CD z danymi (39)
 - Fizyczne błędy nośnika CD (39)
 - o Błędne pliki (Dummy Files) (39)
 - o Płyty CD o pojemności większej niż 74 minuty (Oversized CD) (40)
 - o Błędna wartość TOC (Illegal Table of Contents) (40)
 - o Duże pliki (40)
 - o Programowe (fikcyjne) błędy i inne ingerencje w proces produkcji płyt CD (41)
 - Zabezpieczenia komercyjne (41)
 - o SafeDisc (42)
 - o SecuROM (43)
 - o ProtectCD (43)
 - o Armadillo (The Armadillo Software Protection System) (44)
 - o ASProtect (45)
 - o SalesAgent (46)
 - o VBox (46)
 - Programy napisane w Visual Basicu (46)
 - o Porównanie łańcuchów (47)
 - o Porównanie zmiennych (Variant data type) (48)
 - o Porównanie zmiennych (Long data type) (48)
 - o Przekształcanie typów danych (48)
 - o Przemieszczanie danych (49)
 - o Matematyka (49)
 - o Różne (49)
 - Kolejne poważne błędy obecnych zabezpieczeń (49)

Rozdział 2. Ochrona przed debugingiem (55)

- Stosowane debugery (56)
- Podstawy używania programu SoftICE (56)
 - o Konfiguracja programu (56)
 - o Podstawowe polecenia, funkcje i obsługa (58)
 - Okna (58)
 - Punkty wstrzymania (60)
 - Praca z punktami wstrzymania (63)
- SEH - Strukturalna obsługa wyjątków (64)
 - o Czym jest i do czego służy SEH (64)
 - o Konstrukcje korzystające z SEH (65)
 - o Używane algorytmy (66)
 - Algorytmy wykorzystujące funkcję API CreateFileA (66)
 - Interfejs BoundsChecker i wykorzystanie przerwania INT 3 (67)
 - Wykorzystanie przerwania INT 1 (69)
 - Wykorzystanie przerwania INT 68h (71)
 - Wyszukiwanie wartości w rejestrach (72)
 - Wyszukiwanie wartości w pliku autoexec.bat (72)
- Punkty wstrzymania (73)
 - o Programowe punkty wstrzymania (74)
 - Punkt wstrzymania na przerwanie (BPINT) (74)
 - Punkt wstrzymania na wykonanie (BPX) (75)
 - Punkt wstrzymania na dostęp do zakresu pamięci (BPR) (75)
 - o Sprzętowe punkty wstrzymania (76)
 - Opis przykładowego programu do detekcji sprzętowych punktów wstrzymania (78)
- Metody zaawansowane (80)
 - o Tryby Ring (80)
 - Sposoby przejścia pomiędzy Ring3 i Ring0 (81)
 - o Wykrycie programu SoftICE za pomocą VxDCall (86)
 - o Dezaktywacja skrótu klawiaturowego programu SoftICE (88)
- Kolejne proste możliwości i wykorzystanie SEH (90)

Rozdział 3. Ochrona przed deasemblacją (93)

- Używane deasemblery (93)
- Podstawy użytkowania W32Dasm (94)
- Stosowane algorytmy (96)
 - o Algorytmy podstawowe (97)
 - Ochrona łańcuchów (97)
 - Ochrona importowanych funkcji (97)
 - o SMC - kod samomodyfikujący się (98)
 - Pasywny SMC (99)
 - Aktywny SMC (101)
 - o Edycja kodu programu w trakcie pracy programu (102)

Rozdział 4. Program FrogsICE i obrona przed nim (103)

- Podstawy użytkowania programu FrogsICE (103)
 - Basic options (103)
 - Advanced options (104)

- Stosowane algorytmy (105)
 - o VxDCall funkcji VMM_GetDDBLList (105)
 - o Wykorzystanie funkcji CreateFileA (107)

Rozdział 5. Program ProcDump i obrona przed nim (109)

- Podstawy użytkowania programu ProcDump (109)
- Co to jest dumping i do czego służy (112)
- Używane algorytmy (112)

Rozdział 6. Edycja kodu programu (115)

- Metody stosowane przy edycji kodu programu (115)
- Podstawy użytkowania programu Hiew (116)
 - o Edycja programu do detekcji SoftICE (117)
- Stosowane algorytmy (119)
 - o Kontrola spójności danych (119)
 - Kontrola spójności danych w pliku (120)
 - Kontrola spójności danych w pamięci (122)
 - o Inne sposoby (126)

Rozdział 7. Szyfratory i kompresory PE oraz format PE (127)

- Co to jest format PE pliku? (127)
- Czym jest szyfrator (kompresor) PE i jak działa (128)
 - Jak stworzyć szyfrator (kompresor) PE (129)
 - Wady szyfratorów (kompresorów) PE (130)
- o Stosowane szyfratory (kompresory) PE (130)
 - ASPack (130)
 - CodeSafe (131)
 - NeoLite (131)
 - NFO (131)
 - PE-Compact (132)
 - PE-Crypt (132)
 - PE-Shield (133)
 - Petite (133)
 - Shrinker (134)
 - UPX (134)
 - WWPack32 (135)
- Format plików PE (135)
 - o Weryfikacja formatu PE (135)
 - o Nagłówek PE (138)
 - o Tabela sekcji (140)
 - Nie wiesz, co oznaczają słowa Virtual, Raw i RVA? (141)
 - o Tabela importów (142)
 - o Tabela eksportów (145)
- Tworzymy szyfrator PE (146)
 - o Dodanie nowej sekcji do pliku (147)
 - o Przekierowanie strumienia danych (150)
 - o Dodanie kodu do nowej sekcji (151)

- o Skok z powrotem i zmienne (152)
- o Funkcje importowane (156)
 - Utworzenie tabeli importów (157)
 - Przetworzenie oryginalnej tabeli importów (160)
 - Użycie importowanej funkcji (164)
- o Obróbka TLS (165)
- o Szyfrowanie (167)
 - Jaki wybrać algorytm szyfrowania (167)
 - Znane algorytmy szyfrowania (167)
 - Co się stanie, gdy ktoś złamie szyfr (169)
 - Co szyfrować, a czego nie (170)
 - Demonstracja prostego szyfrowania w szyfratorze PE (171)
- o Finalna postać stworzonego szyfratora PE (175)
- o Dodatkowe możliwości zabezpieczeń (192)
 - Anti-SoftICE Symbol Loader (192)
 - Kontrola Program Entry Point (193)
- o RSA (193)
 - Przykład zastosowania RSA (196)
- o Podsumowanie szyfratorów i formatu PE (197)

Rozdział 8. Kolejne programy stosowane przez crackerów (199)

- Registry Monitor (199)
- File Monitor (201)
- R!SC'S Process Patcher (202)
 - Polecenia w skryptach (203)
- The Customiser (204)

Rozdział 9. Crackujemy (207)

- Cruehead - CrackMe v1.0 (207)
- Cruehead - CrackMe v2.0 (210)
- Cruehead - CrackMe v3.0 (211)
- CoSH - Crackme1 (214)
- Mexelite - Crackme 4.0 (215)
- Immortal Descendants - Crackme 8 (216)
 - Easy Serial (217)
 - Harder Serial (218)
 - Name/Serial (218)
 - Matrix (219)
 - KeyFile (219)
 - NAG (220)
 - Cripple (220)
- Duelist - Crackme #5 (220)
 - Ręczne deszyfrowanie pliku (221)
 - Zmiany bezpośrednio w pamięci (224)
- tC - CrackMe 9 <id:6> (225)
 - Uzyskanie poprawnego numeru seryjnego (225)
 - Zamiana programu na generator numerów seryjnych (227)
- tC - CrackMe 10 <id:7> (228)

- tC - Crackme 13 <id:10> (229)
- tC - Crackme 20 <id:17> (231)
- ZemoZ - Matrix CrackMe (234)
- ZemoZ - CRCMe (237)
 - Edycja programu w edytorze heksadecymalnym (239)
 - Wykorzystanie programu ładującego (242)

Rozdział 10. Kolejne informacje o crackingu (245)

- Wielki wybuch, czyli jak się to wszystko zaczęło (245)
- Kto poświęca się crackingowi (246)
- Znani crackerzy i grupy crackerskie (246)
 - +HCU (247)
 - Immortal Descendants (247)
 - Messing in Bytes - MiB (248)
 - Crackers in Action - CiA (248)
 - Phrozen Crew (248)
 - United Cracking Force - UCF (249)
 - Ebola Virus Crew (249)
 - TNT (249)
 - Evidence (249)
 - Da Breaker Crew (250)
- Ważne miejsca i źródła w internecie (250)
- Kilka ogólnych rad od crackerów (252)
 - Cracking (Lucifer48) (252)
 - NOP Patching (+ORC) (253)
 - Patching (MisterE) (253)
 - Myśleć jak cracker (rudeboy) (253)
 - Tools (rudeboy) (253)

Rozdział 11. Referencje (255)

- Podstawowe instrukcje asemblera (255)
- Komunikaty Windows (261)
- Dostęp do rejestrów (264)
- Przegląd funkcji programu SoftICE (267)
 - Ustawianie punktów wstrzymania (267)
 - Manipulowanie punktami wstrzymania (268)
 - Wyświetlanie i zmiany w pamięci (268)
 - Wyświetlenie informacji systemowych (268)
 - Polecenia dla portów we-wy (270)
 - Polecenia sterujące przepływem danych (270)
 - Tryby pracy (270)
 - Polecenie wydawane przez użytkownika (270)
 - Użyteczne polecenia (271)
 - Polecenia klawiszy w edytorze liniowym (271)
 - Przewijanie (272)
 - Polecenia do manipulowania oknami (272)
 - Obsługa okien (272)
 - Polecenia dla symboli i źródeł (273)

- Operatory specjalne (273)
- Skoki warunkowe, bezwarunkowe i instrukcje set (273)
 - Skoki warunkowe (przejęto z CRC32 Tutorial #7) (273)
 - Skoki bezwarunkowe (przejęto z CRC32 Tutorial #7) (275)
 - Instrukcje SET (AntiMaterie) (276)
- Algorytm CRC-32 (277)
- Kolejne algorytmy do zastosowania z szyfratorami i kompresorami PE (279)
- Demonstracja algorytmu szyfrującego (280)
- Drobne poprawki do ProcDumpa (284)
- Interfejs BoundsChecker (287)
 - Get ID (287)
 - Set Breakpoint (288)
 - Activate breakpoint (288)
 - Deactivate Lowest Breakpoint (288)
 - Get Breakpoint Status (288)
 - Clear Breakpoint (288)

Rozdział 12. Podsumowanie (289)

Skorowidz (291)